PERFORMANCE WORK STATEMENT (PWS)

FOR

COMMAND INFORMATION MANAGEMENT SYSTEM III (CIMS III) SERVICES

4 January 2017

CONTENTS

1.0 SCOPE: The Basic Contract will provide Department of Defense (DoD) agencies with non-commercial integrated Information Technology (IT) solutions. Integrated solutions are comprised of some or all components described in this PWS, and may be tailored to meet agencies' mission needs. Work may be performed on-site or off-site as specified in each Task Order (TO), to provide a variety of IT solutions and support services, including new and emerging technologies that will evolve over the life of the Basic Contract. This PWS provides a general depiction of the types and kinds of non-personal services that may be ordered. Specific services required will be further detailed in individual TO's, as requirements are defined. This contract will be an Indefinite Delivery/Indefinite Quantity (IDIQ) contract.

1.1 The U.S. Army Space and Missile Defense Command/Army Forces Strategic Command (USASMDC/ARSTRAT) serves as the Army Service Component to United States Strategic Command (USSTRATCOM), conducts space operations and provides planning, integration, control and coordination of Army forces and capabilities in support of USSTRATCOM missions. It serves as proponent for Space and Ground based Midcourse Defense (GMD); is the Army operational integrator for global missile defense; and conducts mission related research, development, and acquisition in support of Army Title 10 responsibilities.

1.2 The G6 is responsible for providing Information Management (IM) support to all USASMDC/ ARSTRAT elements. The G6 functions as the staff advisor to the USASMDC/ARSTRAT for all Information Mission Area (IMA) disciplines and is the person charged with planning, engineering, operation, sustainment, and life cycle management of the IMA resources. IM Support Services (IMSS) includes automation, telecommunications, visual information, and sustaining base network infrastructure.

1.3 Non-Personal Services. The contractor shall provide all personnel, supplies, materials, facilities, and equipment (other than that which is stated as Government Furnished). The contractor shall support all functional areas to include, but not limited to: Program Management, Engineering and Development Operations, Help Desk, Video Teleconference Operations, Telecommunications, Network Administration Operations (Infrastructure), Systems Administration Operations (Computer Ops), Configuration Management, Cybersecurity Planning and Operations, Software Development/Management, Maintenance, Systems Integration and Maintenance, Electronic Security Systems/Monitoring and Special Projects. In particular, these efforts will require proficiency with CITRIX/Embedded Zero Client and CISCO networking technologies. These efforts will require a professionally skilled, well-trained, and retainable workforce. TOs may be written for any area or all areas.

1.4 This contract is primarily to support, but is not limited to, the following locations: USASMDC/ARSTRAT-Huntsville – Redstone Arsenal, Alabama; USASMDC/ARSTRAT-Colorado Springs – Peterson AFB, Colorado; Future Warfare Center (FWC), and US Army Kwajalein Atoll/Reagan Test Site (USAKA-RTS) Operations Center – Huntsville (ROC-H). Additional organizations within DoD may also utilize this contract for IT support determined to

be within scope. Organizations outside of the command should contact the contract-level COR if interested in inquiring about obtaining a TO.

1.5 All efforts and support shall follow guidelines, regulations, and policies specified in individual TO's. In the event of conflict between the documents referenced and the contents of this PWS or of the TO PWS, the contents of the TO PWS(s) shall take precedence. Clarification and guidance shall be the responsibility of the contractor in understanding what is requested in this PWS and associated documents. The contractor shall seek clarification from the Contracting Officer (KO) or COR in areas not understood. In disputes between the contractor and the Government involving interpretation of the PWS, only the KO has the authority to render a final interpretation. CORs and TO CORs do not have authority to interpret the PWS.

2.0 GENERAL INFORMATION:

2.1 Performance Work Statement: The PWS describes a performance based work environment in terms of "what" the required service output is, rather than "how" the work is to be performed. The contractor shall be part of a quality customer-focused multifunctional team that meets all IT needs identified in a TO. The contractor shall provide all supervision, personnel, equipment, supplies, transportation, tools, materials and other items and non-personnel services, not provided by the customer necessary to perform all tasks and functions as defined in the PWS and TO. The contractor is required to manage the quality of the services delivered using their internal management structure. The PWS strives to create a government-contractor relationship that promotes achievement of mutually beneficial goals, and promotes a partnership environment.

2.1.1 Specific performance requirements will be set forth and funded on individual TO's issued under the basic IDIQ contract. The CIMS III contract will be managed by Space and Missile Defense Center (SMDC)-G6 via a contract-level COR. Individual TO CORs will be assigned under individual TO's.

2.2 Periods of Performance (PoP): The Ordering PoP for the Basic Contract shall begin ____ and continue up to ____. Each TO issued under the Basic Contract shall specify the TO PoP, to include any options.

2.3 Contracting Officer's Representative (COR) and Task Order CORs (TO COR): The KO will delegate, in writing, COR(s) and TO COR(s) with the authority for inspection and acceptance of services for each TO.

2.4 Core Hours of Operation: Unless otherwise specified in individual TO's, the contractor shall ensure adequate technical expertise is available to provide responses to specific tasks based on a normal 40-hour work week, Monday-Friday, 0700-1730 local time. During key events and operational missions, contractor services may be required for up to 24 hours per day, 7 days per

week (including holidays). All support personnel scheduled to work shall be present and actively providing support during the hours specified. The Government will not require the contractor to work over their regular 40-hour work week. Some personnel may need to work flex time to ensure coverage during core hours of operation. Routine overtime will not be authorized. If a situation arises where the contractor feels overtime may be necessary, this shall be discussed with and approved by the KO and TO COR.

2.5 Federal Holidays: The following Federal Holidays are observed by USASMDC/ARSTRAT and authorized for contractors during performance of the contract:

New Year's Day
Martin Luther King's Birthday
Presidents Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veterans Day
Thanksgiving Day
Christmas Day

2.6 Service Support During An Emergency: In addition to routine operational support, the contractor may be required to respond to emergency work requests in support of contingency operations. In certain instances, special emergency contact lists may be required as requested by the COR (i.e., after hours support list, essentials listing, etc.)

2.7 Continuation of Essential Contractor Services: The contractor may be required to perform services during a crisis per the contractual requirements in support of a specific TO. If the contractor is required to perform the contractual requirements on a modified schedule, the modified schedule will be provided by the KO and TO COR. Services shall continue unless otherwise directed by the KO.

2.7.1 Mission Essential Personnel: The contractor may be required to ensure personnel necessary to accomplish tasks designated as "mission essential" report to assigned work locations (or Government Continuity of Operations Plan (COOP) designated facilities) and perform required tasks, regardless of weather or security conditions. The Government will identify tasks qualifying performers as essential personnel in TO language, and the contractor shall provide a list of essential personnel required to perform those tasks to TO COR's. TO COR's will be responsible for providing Government security personnel with the list of contractor "mission essential personnel" to enable continued access to Government facilities when "non-essential" personnel are barred. The contractor shall operate in accordance with

(IAW) DoD Instruction (DoDI) 3020.37, Continuation of Essential DoD Contractor Services During Crisis.

2.7.2 Non-Essential Personnel: All personnel not specifically designated as "mission essential personnel" are considered "non-essential" personnel. During periods of inclement weather or other emergencies when Government-provided office space is closed by the Government for non-essential personnel, contractor employees may direct/authorize non-essential contractor personnel to work at company-provided locations or telecommute, if duties allow, and they are directly charged to the contract. In the event written contractor policy is to provide administrative leave, instead, such time shall not be directly chargeable to the contract, but may be included in overall labor rates as an employee benefit.

2.8 Contractor Personnel: The contractor shall not employ people for work on the contract who are potential threats to the health, safety, security, general well-being, or operational mission of the installation and its population. All contract employees shall be United States (U.S.) citizens, hold United States government security clearances, and possess local designated access approvals per the direction of the customers' security and Cybersecurity guidelines. The contractor shall not use non-U.S. citizens to perform any work under this contract. All employees shall be able to understand, read, write, and fluently speak the English language.

2.8.1 Employee Identification: All contractor personnel shall be required to wear company identification badges so as to distinguish themselves from Government employees. Where available, contractor employees shall wear Government-issued access badges with coloration that distinguishes contractors from Government employees and "contractor" designation clearly displayed on the badge. These badges must be visible at all times when working within Government facilities. In order to obtain a contractor badge, the contractor shall ensure coordination takes place with the proper agency office. When conversing with Government personnel during business meetings, over the telephone or via electronic mail, support contractor personnel shall identify themselves as such to avoid any perception that they may be Government employees and to avoid situations arising where sensitive topics might be better discussed solely between government employees. Electronic mail signature blocks shall identify contractor/company affiliation. Documents or reports produced by contractors shall be suitably marked as contractor produced products or contractor participation appropriately disclosed. Contractor personnel occupying collocated space in a Government facility shall identify their workspace area with their name and company/contractor affiliation.

2.8.2 Supervision of Employees: The contractor shall not allow Government employees to supervise contractor employees or direct work outside the limits of this contract or TO. Likewise, the contractor shall not supervise or otherwise direct government employees, nor shall the contractor supervise or direct employees of other contractors outside the contractors' own subcontracting/teaming arrangements. The contractor shall ensure that all support provided to the Government is coordinated, approved, and directed by contractor task leads and that their

subordinate employees do not work directly or constructively for Government employees in an "employee-like" relationship that could result in personal services.

2.8.3 Third Party Contractors: The contractor is expected to cooperate with third party contractors in the capacity of their duties under this contract.

2.8.4 Key Personnel: The contractor's key personnel shall demonstrate adequate levels of recent and relevant expertise for the functional areas identified. Each TO shall provide special requirements if needed. The contractor shall furnish in writing to the KO and COR the cell phone numbers and/or telephone numbers of key management personnel such as the Contract Manager, Program Manager, alternate(s) and any other applicable personnel no later than fifteen (15) business days prior to contract start. The contractor may be required to furnish in writing to the KO and COR the names, position, labor category, and phone numbers of all key personnel as specified in the TO. The KO and COR shall be notified in writing immediately whenever changes are made to key personnel.

2.8.4.1 Prior to permanently reassigning any key personnel, the contractor shall provide the KO not less than thirty (30) days advance notice and shall submit justification (including proposed substitutions) in sufficient details to permit evaluation of the impact on the contract. No reassignment shall be made by the contractor without written consent of the KO. The "Key Personnel" list may be amended from time to time during the course of the contract to either add or delete personnel, as appropriate.

2.8.5 Program Management: A Program Management system should exist to oversee, direct, and coordinate all contract and TO support activities. The contractor shall provide a senior-level point of contact (POC) i.e. Program Manager with a professional background in all aspects of IT who shall be responsible for the performance of the work specified in this contract and applicable TO's. An alternate is required to act for the contractor when the POC is absent. Program Managers shall be Project Management Professional (PMP) certified. The POC provides overall management of TO's, projects, cost and budgets, personnel, planning, quality control, direction, coordination, deliverable submissions, effort proposals, and reviews necessary to assure effective contract performance and acts as single POC for the KO and COR on these and related issues. The POC shall be required to possess a TOP SECRET (TS) clearance or be eligible for immediate adjudication by the cognizant security authority upon award of the contract. The POC may eventually require a Sensitive Compartmented Information (SCI) clearance to provide Sensitive Compartmented Information Facility (SCIF) Operations Support. The POC shall control contractor personnel and monitor support to ensure employees are not performing Inherently Governmental Functions (IGF) or personal services on any effort, reporting such taskings to the KO and COR for clarification and validation prior to acceptance or accomplishment of such work.

2.8.5.1 Authority: The POC and alternate shall have full authority to commit the contractor on all matters relating to the performance of the contract.

2.8.5.2 Availability: The POC or alternate shall be available within two hours (by phone, Video Teleconference (VTC), or in person) for any contract-level issues. Availability requirements may vary among individual TO's and will be specified in the TO if different from this paragraph.

2.8.6 Specialized Experience:

2.8.6.1 The contractor shall ensure their personnel are fully qualified and trained. The contractor shall provide personnel with the requisite knowledge, skills and abilities to successfully support this requirement to include formal education levels, proper certifications, additional certified training, hands-on training, and past job experience necessary to satisfy their assigned area(s) of responsibility. The technical as well as management personnel shall be fully qualified with requisite certificates, degrees, courses, education, expertise and/or work experience that apply directly to work being performed. Additional training necessary to improve the knowledge, skills and abilities of personnel designated by the contractor to support this effort is the responsibility of the contractor and shall not take place during core hours or at a cost to the Government.

2.8.6.2 Cybersecurity/IT Certification: Per DoD 8570.01-M, Defense Federal Acquisition Regulation (DFARS) 252.239-7001 and Army Regulation (AR) 25-2, the contractor employees supporting Cybersecurity/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

2.8.7 Employment of Government Employees: The contractor shall not employ any person who is an employee of the United States Government if the employment of that person would create a conflict of interest, or the appearance of a conflict of interest. Furthermore, the contractor shall not employ any person who is an employee of the Department of the Army, either military or civilian, unless such person seeks and receives proper approval. The contractor is prohibited from employing off-duty Government personnel who are managing any contracts or subcontracts awarded to the contractor.

2.8.8 Hiring Military Personnel: Prior to offering a position to a member of our active duty personnel, the contractor shall provide the KO not less than thirty (30) days advance notice to permit evaluation of the impact of this assignment. No reassignment of this type shall be made by the contractor without written consent of the KO.

2.8.9 Off-Duty Active Duty Military: The contractor is cautioned that off-duty active military personnel hired for the contract/TO may be subject to permanent change of station, change in duty hours, or deployment. Military Reservists and National Guard members may be

subject to recall to active duty. The abrupt absence of these personnel could adversely affect the contractor's ability to perform; however, their absence at any time shall not constitute an excuse for non-performance.

2.9 Security: Personnel employed by the contractor in support of this effort shall be required to have the minimum of a SECRET security clearance, unless KO approves interim SECRET security clearance. In some instances, the contractor shall be required to obtain a TS or TS/SCI clearance as specified by the TO. The contractor shall also be required to have a current TS facility clearance. If required, the contractor shall maintain full accountability and tracking of all clearances and shall work with the COR and designated Cybersecurity personnel in maintaining such status. While operating at a Government facility the contractor shall abide by security procedures and as identified in each TO.

2.9.1 Network Clearances: The work to be performed on this contract will usually be "Sensitive but Unclassified" but some work may be SECRET.

2.9.2 Government Facility Access: Upon TO start and hiring of new employees, the contractor will be required to obtain Common Access Cards (CAC) and badges required for personnel to access Government work locations and computer systems. Specific contractor security access requirements will be outlined in the Contract Security Classification Specification, DD Form 254 for the TO. Access to Government-controlled computers and locations will be required for most employees. The Government will not provide access to any Government facilities on Government holidays, except when Government employees associated with contractor work are also required to work.

2.9.3 Physical Security: The contractor shall safeguard all government property and controlled forms. At the close of each work day/period, facilities, support equipment, and materials shall be secured. The contractor shall immediately report all thefts, vandalism, or destruction of government-owned property and/or equipment to the COR upon discovery.

2.9.4 Key/Access Badge Control: The contractor may be required to obtain access badges to gain unescorted entry into various Government facilities. Access badges are typically unique to an area and a single badge may not be sufficient to gain access all Government facilities supporting on this contract. The contractor shall immediately report to the TO COR any occurrences of lost, unauthorized uses, or unauthorized duplication of keys or access badges. In the event keys or access badges are lost or duplicated, the contractor may be required, upon written direction of the KO to re-key or replace the affected lock(s) or access badges. The government may, at its option, replace the affected lock(s), access badges or perform re-keying and deduct the cost of such from the monthly payment due to the contractor.

2.9.5 Army Training Certification Tracking System (ATCTS): All contractor employees with access to a government information system (IS) must be registered in the ATCTS at

commencement of services, and must successfully complete the DoD Cybersecurity Awareness Challenge prior to access to the IS and then annually thereafter.

2.9.6 Access and General Protection/Security Policy and Procedures: This paragraph applies to contractor employees with an area of performance within an Army controlled installation, facility or area. The contractor and all associated sub-contractor employees shall comply with applicable installation, facility and area commander installation/ facility access and local security policies and procedures (provided by government representative). The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. The contractor workforce must comply with all personal identity verification requirements as directed by DoD, Department of the Army Headquarters (HQDA) and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

2.9.7 Contracts That Require Handling or Access to Classified Information: Contractor personnel may have access to classified documentation, networks and discussions. The contractor shall be responsible for the proper handling of such information in all forms. The contractor shall comply with Federal Acquisition Regulation (FAR) 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); any revisions to DoD 5220.22-M, notice of which has been furnished to the contractor.

2.9.7 Courier Service: Contractor may be required to transport (Secret) classified material from one location to another via secure means in support of task requirements. Contractors transporting classified material must obtain the appropriate courier training prior to transporting classified Information. In most cases, the information will be transported via digital media such as, hard drive or Compact Disk (CD), but may include printed material and will be protected and secured in a Government approved container. Courier Service shall be conducted IAW: *DoD 5220.22*, and:

2.9.7.1 Be properly briefed on courier responsibility to safeguard classified information.

2.9.7.2 Possess an identification card or badge which contains the contractor's name and the name and a photograph of the employee.

2.9.7.3 Ensure all classified material being transported will remain in their possession at all times throughout the travel. If necessary, arrangements shall be made in advance of departure

for overnight storage at a U.S. Government installation or at a cleared contractor's facility that has appropriate storage capability.

2.9.7.4 Ensure all hand carried classified material is inventoried by a Government official prior to departure and a copy of the inventory shall be carried by the designated courier. Upon return of the courier to the originating facility, an inventory of the classified material shall again be made, as confirmation and receipt of classified material the courier was charged.

2.10 Training:

2.10.1 Government-Mandated Training: Contractor employees may be required by the Government to attend Government-mandated training in order to work on this contract. If required, such training shall be accomplished during normal duty hours and charged to the contract as part of performance of normal duties. Attendance at training sessions does not relieve the contractor from providing support as required by the TO. If any government approved costs are incurred by the contractor for government-mandated conferences/training, actual costs may be reimbursed on a case-by-case basis at the discretion of the KO.

2.10.2 Utilization of Government Computers/Systems:

2.10.2.1 Anti-Terrorism (AT) Level I Training: All contractor employees, to include subcontractor employees, requiring access to Army installations, facilities and controlled access areas shall complete AT Level I awareness training within ten (10) calendar days after performance start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR and TO COR, within ten (10) calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: https://atlevel1.dtic.mil/at.

2.10.2.2 iWATCH Training: The contractor and all associated subcontractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity Anti-Terrorism Office (ATO)). This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR or TO COR. This training shall be completed within thirty (30) calendar days of contract award and within thirty (30) calendar days of new employees commencing performance. Report results to the COR No Later Than (NLT) ten (10) calendar days after completion of training. This training is also required on all USASMDC/ARSTRAT TO's.

2.10.2.3 Cybersecurity/IT Training: All contractor employees and associated sub-contractor employees must complete the DoD Cyber Security Awareness Challenge training before issuance of network access and annually thereafter. All contractor employees working Cybersecurity/IT privilege level functions must comply with DoD and Army training

requirements in DoD 8570.01-M and AR 25-2.

2.10.2.4 The contractor shall ensure contract employees are certified IAW industry standards and DoD Directive (DoDD) 8570.01-M.

2.10.2.5 Personal Identifiable Information (PII) Training: All contractor employees and associated sub-contractor employees must complete the PII/DoD Component Privacy Act Training annually IAW DoD 5400.11-R – DoD Privacy Program. Training results shall be reported in the Monthly Status Report (MSR) (refer to paragraph 4.1.2 in this PWS).

2.10.3 Contractor Maintained Qualifications and Training: It is the responsibility of the contractor to provide properly trained, skilled employees. The contractor shall ensure that contractor employees maintain suitable and adequate qualifications. Individual employees may also require special technical training to achieve skills needed to accomplish assigned tasks. Skills advancement training will be at contractor expense and does not relieve the contractor from providing ongoing support required by the PWS. The government will not reimburse the contractor for normal and necessary training required to perform work under the PWS.

2.11 Quality Control (QC):

2.11.1 Quality Control Plan (QCP): The contractor shall be responsible for overall responsiveness, cost control, adherence to schedules, technical quality of work, management of contractor's team efforts and commitment to customer satisfaction. The contractor shall establish a process to provide an accurate assessment of performance in all areas of the contract and implement a quality program through the QCP.

2.11.2 Contractor personnel assigned to maintain the QC program shall perform independently of personnel assigned to other TO deliverables.

2.11.2.1 QC personnel shall have sufficiently well-defined responsibility, authority, and the organizational freedom to identify and evaluate quality problems in order to initiate, recommend, and/or provide solutions.

2.11.2.2 QC personnel shall maintain adequate records of any audits, inspections, and tests to support the conformance to the requirements and effective operation of the quality program.

2.11.2.3 QC personnel shall ensure timely and effective corrective action is obtained for all deficiencies identified by the contractor or by the Government. All deficiency responses shall include the cause of the deficiency to preclude recurrence and an analysis of the quality program's effectiveness in the area of the deficiency.

2.11.2.4 The QCP shall be submitted to the KO for acceptance no later than fifteen (15)

business days after contract award, and within five (5) business days of any changes.

2.11.2.4.1 The QCP shall include the methods that the contractor will utilize in order to ensure their internal quality control is implemented and followed so that each of the requirements of the PWS are met.

2.11.2.4.2 Address the methods to be used by the contractor for identifying and preventing defects in the quality of service.

2.11.2.4.3 Describe the records to be kept to document inspections and corrective or preventive actions taken.

2.11.2.4.4 Describe the comprehensive management program used by the contractor to address customer service, corrective actions, employee standards of dress, conduct/behavior and efforts that foster a healthy working relationship between the government and the contractor.

2.12 Safety Requirements and Precautions: Contract activities will be conducted in a safe and healthful manner that minimizes accidents as well as impacts on Army operations and members of the public. Contractors must comply with applicable Federal, State, and local codes, standards, and laws.

2.12.1 Incident/Mishap Reporting: In the event of a safety incident/mishap, immediately report the incident to the COR and TO COR. If the government elects to conduct an investigation, the contractor shall cooperate fully and assist government personnel until completed.

2.12.2 The contractor shall comply with the Department of Labor Occupational Safety and Health Act standards, Title 29, Code of Federal Regulations (CFR), Part 1910, Life Safety Code, and agency policies and regulations.

2.12.3 The government provided facilities shall be made available for government safety inspections upon request.

2.13 Travel: The contractor shall perform temporary duty (TDY) non-local travel (Continental United States [CONUS] and Outside the Continental United States [OCONUS]), as required by the contract and as stated in individual TO's during the performance of this PWS.

2.13.1 The Government will not reimburse the contractor for local travel performed within 50 miles of the usual place of performance of the work against a particular PWS requirement.

2.13.2 If travel is required, the contractor shall submit all travel requests and security clearance information to the Government TO COR for review and approval, at least two weeks

prior to the date the required travel is to begin. A copy of the request and approval will be sent to the KO. Emergency (last minute) travel requirements shall be coordinated as above by telephone or fax, if necessary. All travel costs shall be charged to the reimbursable Travel Contract Line Item Number (CLIN), and the contractor shall verify sufficient funds are loaded in that CLIN when requesting approvals.

2.13.3 The government will reimburse the contractor for government required pre-approved travel necessary for the performance of the contract. Per Diem and other travel costs will be reimbursed IAW FAR Part 31. Reimbursement for contractor travel shall be limited to entitlements listed in the Joint Federal Travel Regulation (JFTR). Cost for delays in route (excluding government caused delays) will not be reimbursed.

2.13.4 All supporting documents for reimbursement shall be submitted into Wide Area Workflow (WAWF) for submission with the invoices for the respective travel.

2.14 Phase-In Effort: The contractor may be required to perform phase-in efforts on TO's, and maintain continuity of operations during transition of performance from incumbent contractors. If phase-in is required, the contractor shall take all actions necessary to ensure smooth transition of responsibilities/operations support from the incumbent contractor to the CIMS III contractor. The contractor shall be provided access to the functional area to observe, interface, and work with the existing work force prior to TO start date without disruption of work and operations in progress as specified by the TO. The contractor may be required to coordinate and execute a transition plan ensuring a well-organized and systematic approach.

2.15 Phase-Out Effort: At the end of contract or TO performance, the contractor may be required to phase out the existing contract or TO turning over total contract control to the new contractor in a well-organized, systematic, and planned manner. If required by the TO, the contractor may be requested to provide familiarization to any follow-on contractor. During the phase-out familiarization period, the incumbent contractor shall be fully responsible for operation of all IT services as outlined in the PWS. In the event the follow-on is not awarded to the incumbent, the contractor shall interface and fully cooperate with other contractors and government personnel to the extent required to permit an orderly changeover to the follow-on contractor. The contractor shall not commit any act that will interfere with the performance of work by any other contractor or Government employee. The contractor shall comply with government equipment disposition instructions.

2.16 Contractor Manpower Reporting: The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Department of Army via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/.

2.16.1 Reporting inputs will be for labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013. If the Government approves an extension of the report due date, all data shall be reported no later than (NLT) the extension date. Contractors may direct questions to the help desk at: http://www.ecmra.mil/.

2.17 Compliance with Agency Mandates: It is the responsibility of the contractor to stay abreast of and in compliance with changes, including supplements and amendments. It is the contractor's responsibility to insure that all mandatory publications are accessible to applicable employees and kept up to date. Unless a specific issue date is indicated, the issue in effect on the date of this PWS shall apply. In the event of conflict between this PWS and any mandatory publication document referred to herein, the requirements explicitly stated in this PWS take precedence.

2.18 Intellectual Property/Data Rights:

2.18.1 Intellectual Property: In the event that the contractor, while supporting the TO requirements, seeks ownership, copyright, or patent of inventions, computer software, computer documentation, technical data or other contractor-developed innovations and initiatives under the applicable intellectual property laws and regulations, the Contactor will promptly notify the KO in writing. Further, if the contractor determines to use technical data, copyrighted, or patented items protected by intellectual property rights in performance and to be delivered to the Government, the contractor shall notify the KO as soon as possible.

2.18.2 Distribution Control of Technical Information:

2.18.2.1 The following terms applicable to this clause are defined as follows:

(1) Technical Document: Any recorded information that conveys scientific and technical information or technical data. This includes such informal documents as working papers, memoranda, and preliminary reports when such documents have utility beyond the immediate mission requirement or will become part of the historical record of technical achievements.

(2) Scientific and Technical Information: Communicable knowledge or information resulting from or pertaining to conducting and managing a scientific or engineering research effort.

(3) Technical Data: Recorded information, regardless of form or method of the recording, of a scientific or technical nature (including computer software documentation) as defined in DFARS 252.227-7013(a)(14), 7015(a)(5), and 7018(a)(20). The term does

not include computer software or data incidental to contract administration, such as financial and/or management information.

2.18.2.2 The distribution of any technical document prepared under this contract, in any stage of development or completion, is prohibited without the approval of the KO and all technical documents prepared under this contract shall initially be marked with the following distribution statement, warning, and destruction notice:

(1) DISTRIBUTION STATEMENT F – Further dissemination only as directed by USASMDC/ARSTRAT KO (date of determination) or higher DoD authority.

(2) WARNING – This document contains technical data whose export is restricted by the Arms Export Control Act (22 U.S.C.§2751 et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq), as amended. Violation of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoDD 5230.25.

(3) DESTRUCTION NOTICE – For classified documents, follow the procedures in DoD 5200.22-M, National Industrial Security Manual, Chapter 5, Section 7, or DoD 5200.1-R, Information Security Program Regulation, Chapter IX. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

2.18.2.3 As a part of the review of preliminary or working draft technical documents, the Government will determine if a distribution statement less restrictive than Statement F specified above would provide adequate protection. If so, the Government's approval/comments will provide specific instructions on the distribution statement to be marked on the final technical documents before primary distribution.

2.18.2.3.1 The contractor shall place distribution statement conspicuously on all technical documents regardless of media or format. For standard written or printed material, the distribution statement shall appear on the front cover, title page, and Standard Form (SF) 298, "Report Documentation Page," where applicable. The SF 298 is available at http://www.dtic.mil/whs/directives/forms/index.htm. If the technical information is not prepared in paper form but is prepared digitally or is in any medium that does not have a cover or title page, the applicable distribution statement shall be affixed to all physical and digital items by other means in a conspicuous position for ready recognition. Distribution Statements apply to both Classified and Unclassified technical information.

2.18.2.3.2 The contractor shall use the seven authorized distribution statements providing options ranging from unlimited distribution to no secondary distribution without specific authority of the controlling DoD office. In selecting and applying the appropriate statement, the

contractor shall consider the information contained in the document and the audience for which it is intended.

2.18.2.3.3 Below the list of distribution statements is a list of reasons that the contractor shall use with its corresponding distribution statement. (See example below).

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

DISTRIBUTION STATEMENT B. Distribution authorized to U.S. Government agencies only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).

DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government agencies and their contractors (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).

DISTRIBUTION STATEMENT D. Distribution authorized to DoD and U.S. DoD contractors only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).

DISTRIBUTION STATEMENT E. Distribution authorized to DoD Components only (reason) (date of determination). Other requests for this document shall be referred to (controlling DoD office).

DISTRIBUTION STATEMENT F. Further dissemination only as directed by (controlling office), (date of determination) or DoD higher authority.

2.18.2.3.4 The Government and contractor shall use the following "reasons" for applying distribution statements, as appropriate.

REASON	**A**	**B**	**C**	**D**	**E**
PUBLIC RELEASE	X				
ADMINISTRATIVE OR OPERATIONAL USE: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may apply to manuals, pamphlets, technical orders, and other publications containing valuable technical or operational data.		X	X	X	X
CONTRACTOR PERFORMANCE EVALUATION: To protect information in management reviews, records of contract performance		X			X

evaluation, or other advisory documents evaluating programs of contractors.					
CRITICAL TECHNOLOGY: To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified.		X	X	X	X
DIRECT MILITARY SUPPORT: The document contains export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize an important technological or operational military advantage of the United Stated, another country, or a joint U.S.-foreign program. Designation of such data is made by competent authority IAW DoDD 5230.25.					X
EXPORT CONTROLLED: To protect information subject to the provisions of DoDD 5230.25.		X	X	X	X
FOREIGN GOVERNMENT INFORMATION: To protect and limit distribution IAW the desires of and agreements with the foreign government that furnished the technical information.		X	X	X	X
OPERATIONS SECURITY: To protect information and technical data that may be observed by adversary intelligence systems and determining what indicators hostile intelligence systems may obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.		X			X
PREMATURE DISSEMINATION: To protect patentable information on systems or processes in the development or concept stage from premature dissemination.		X			X
PROPRIETARY INFORMATION: To protect information not owned by the U.S. Government and marked with a statement of a legal property right. This information is received with the understanding that it will not be routinely transmitted outside the U.S. Government.		X			X
TEST AND EVALUATION: To protect results of test and evaluation of commercial products or military hardware when disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.		X			X
SOFTWARE DOCUMENTATION: To protect technical data relating to computer software that is releasable only IAW the software license in subpart 227.72 of Title 48 of the CFR.		X	X	X	X
SPECIFIC AUTHORITY: To protect information not specifically included in the above reasons, but which requires protection IAW valid documented authority (e.g., Executive orders, statutes such as Atomic		X	X	X	X

Energy Federal regulation). When filling in the reason, cite "Specific Authority (identification of valid documented authority)."					
VULNERABILITY INFORMATION: To protect information and technical data that provides insight into vulnerabilities of U.S. critical infrastructure, include DoD warfighting infrastructure, vital to National Security that are otherwise not publicly available.		X	X	X	X

2.18.3 Technical Data Rights: When the contractor asserts title and rights for technical data under this contract, the Government will invoke DFARS 252.227-7013 and reach an agreement with the contractor on its licensing rights.

2.18.4 Software License: In addition to the rights stipulated in DFARS 252.227-7014 clause hereof, when software is to be delivered with other than unlimited rights in the Government, the contractor shall obtain all such software licenses in the Government's name. In addition to other rights stated in this contract, it is agreed that the Government shall have the right to re-host software on the computer of a Government contractor.

2.18.5 Rights in Special Works: When the Government must own or control copyright in all works or portions of work first produced, created, or generated under this contract, the Government will invoke DFARS 252.227-7020, Rights in Special Works. The contractor shall assign copyright in those works to the Government and label the work the following notice: "© (Year date of delivery) United States Government, as represented by the Secretary of Army. All rights reserved." The Government will have unlimited rights in the special works, and the contractor grants to the Government licenses in accordance with the DFARS clause. In addition, the contractor hereby relinquishes any rights to use or disclose such works beyond what is required by the contract.

3.0 DESCRIPTION OF SERVICES: The contractor shall provide IT related services to support agencies' IT requirements. The following services are examples of work that might be performed. This list is not meant to be all-inclusive, but rather general indications of the types of services within a given category. Other services not listed as examples which adhere to the definition for each section may also be within scope. When in doubt about scope or simply to be cautious, contact the COR/KO for a scope determination.

3.1 Program Management: Program Management services include development and implementation of standard methodologies and automated process management systems; IT management providing support for operations and IT resource management requirements; supporting strategic planning, management, and control functions integral to IT initiatives; providing foundational support to effectively align IT requirements with an agency's mission operations; enabling the development and implementation of enhanced governance capabilities; oversee, direct, and coordinate IT engineering program upgrades and performance improvement

programs by designing, developing, re-engineering, and integrating state-of-the-art software and hardware enhancements.

3.2 Operations Management and Support: Operations Management and Support services include planning, coordination, command, control, critical issues and priorities, re-engineering, support, and especially daily workflow as specified in the TO's. The contractor shall support systems involved in routine day-to-day operations and training.

3.3 Network Administration (Network Operations): Network Administration services include installing and maintaining network and terminal equipment such as routers, switches, encryption devices, and Channel Service Units (CSU); assist in establishing, and maintaining a network operations capability; providing network support to customer programs and activities, both local and remote; providing network technical support for telecommunications protocols; recommending upgrades; providing technical support for network physical layers; provide network management support for local area networks (LAN); providing technical support for the design, development and implementation of new LANs and for the expansion of existing networks; installing network hardware and software; system testing; monitoring and maintaining developing application enhancements; and providing technical support for the design, development and implementation of Wide Area Networks (WAN).

3.4 Systems Administration (Computer Operations): Systems Administrations (Computer Operations) services include implementing and maintaining a Computer Operations capability; implementing and maintaining Server Operations; managing and operating enterprise servers and support equipment; daily operations of the customer's networks, enterprise, e-mail servers and e-mail remote capabilities; enterprise server virtualization; networked printer operations; monitoring and coordination of telecommunications networks and associated equipment; backup operations; disk management/operations; input/ output control; job control, and related tape library functions; operating systems analysis and support; migrating efforts to the latest release of operating system software; modifying system software; developing routines for systems-level functions which include system security; system status and performance monitoring; system performance tuning and enhancement; inter-system communication and data transfer; user interfaces; and peripheral interfaces.

3.5 Technical Support: Technical Support services include ensuring full operations and integration with information management systems and customer/user support functions; managing and controlling all IT computer resources; being responsive to Chief Information Officer(G6) direction and priorities; identifying negative IT issues and impacts (i.e., processes, procedures, aging IT elements, ineffectiveness, obsolete elements, defectiveness, and any IT components that may affect the quantitative or qualitative value of service provided by this contract); properly identifying issues; providing informative and valid information; proposing resolutions; providing an effective Reengineering and Life Cycle Management program; and network Configuration Control.

3.6 Help Desk Operations: Help Desk Operations services include establishing and maintaining a centralized Help Desk Operations system; providing technical and application assistance support to agency customers for IT equipment and services; assisting customers with resolution of application, software, hardware, network, training coordination, and other IT related problems; providing Tier 1 and Higher Level Tier support; providing hardware/software maintenance, configuration management and hands-on trouble-shooting; resolving hardware/software problems for end-user systems; installing hardware and software; configuring end-users' personal computers (PCs)/laptops/Zero Client/ notebooks, ensuring all applications work properly; also ensuring that each system conforms to the standard configuration and are security compliant within the command; update and maintain databases.

3.7 Video Teleconference (VTC) Operations: VTC Operations services include organizing, configuring, set-up, transporting and operating all necessary equipment supporting VTCs, conference rooms, communications, engineering, technical support, trouble-shooting, audio, projections, operations, multimedia, maintenance, installation, fine-tuning, facilitation, scheduling, operations, dialup assistance, switchable interfaces, mixers, controlling devices, cameras, portable VTC systems microphones, audio/video interfaces, control consoles, and training, and providing hands-on training to systems users. The contractor shall ensure the required Defense Information Systems Agency (DISA) Video Services (DVS) Level II certification is obtained prior to award of any VTC TO.

3.8 Telecommunications: Telecommunication services include establishing and maintaining a telecommunications operation capability; managing all technical aspects of the customer's communication operation; technical assistance and support for wireless and stationary communication equipment. Telecommunications Operations may include Private Branch Exchange (PBX) Administration; installation, configuration, and maintenance of analog and digital telephone line databases; maintain voice mail and conferencing bridge; communications wiring infrastructure; multi-media interface floor boxes; Government/ARMY issued handheld wireless devices, operations and specialized mobile communications devices with data capabilities.

3.9 Integration and Restoration: On-demand Automated Information Systems (AIS) integration and restoration; with emphasis on Network inside wiring/cabling and infrastructure, VTC/Multimedia systems and suites, large display operations center and other critical AIS, components and mission systems.

3.10 Maintenance Requirements: Maintenance services include scheduled maintenance on IT related equipment; preventive maintenance; non-scheduled (i.e. emergency or on-call) equipment maintenance; software and license maintenance**;** application software maintenance; operating systems analysis and software support; migrating operating system software;

modification of system software; integration maintenance support for the network infrastructure; and special systems maintenance for special purpose IT systems.

3.11 Configuration Control/Management: The Configuration Control/Management services include identifying any changes to the enterprise which supports operations consistent with the system architecture and associated policies.

3.12 Cybersecurity Operations: Cybersecurity services include protecting and defending network availability; protecting data integrity; providing the ability to implement effective computer network defense; providing cost effective, timely and proactive Cybersecurity measures and controls. It may also include supporting agency specific Cybersecurity requirements related to qualified personnel with security clearances/background checks; security risk assessments; vulnerability management processes, Risk Management Framework (RMF) system reviews, and plans; installation/configuration of CS systems; creation/modification of documents; and defense of the environment—including hardware & software, the networks, and supporting infrastructure, as dictated by the nature of the information (classified/unclassified) and associated risk.

3.13 Special Project Support: Special Project services include studies involving IT innovations or other IT related subjects; recommendations, development, and re-engineering of existing software applications and architecture supporting the web solutions; and surge requirements.

3.14 Software Engineering: This service includes the concept, design, development, testing, government acceptance, integration, full documentation, and subsequent delivery and operation of all software.

3.15 Software Development/Management: Software development services include gathering, analysis, design, development, testing, control, security, integration, and performance related management, operations, and maintenance; designing/creating SharePoint templates, workflows, and portal branding; portal branding includes graphics and page layout design; providing assistance to users in learning how to update their content on systems such as SharePoint; and creating and maintaining web accessible forms and templates.

3.16 Web Portals and Special Software Systems: Web portals and special software systems services include providing support in the areas of technology enhancements, graphic support, testing, designing and creating; identifying and recommending the latest technologies; web hosting and design capabilities; posting on the server, testing and re-engineering existing web pages; and maintaining web sites.

3.17 Electronic Security Systems (ESS): ESS services comprised of Intrusion Detection Systems (IDS), Access Control Systems (ACS), Closed-Circuit Television (CCTV) systems,

supporting network and electrical infrastructure, and supporting computer servers and/or workstations. ESS operations may include monitoring of currently-installed intrusion alarms in conjunction with an Underwriters Laboratories (UL)-certified Government Contractor Monitoring station (GCMS); performing routine, scheduled maintenance as required by UL; and providing daily and monthly activity reports for all IDS accounts. Perform unscheduled maintenance and repairs of ESS and ACS components and devises, to include diagnosing troubles, repairing or replacing damaged/defective components as required, performing reprogramming/reconfiguration of software and/or hardware components as required, and providing labor, tools, wiring, cabling, parts, and equipment to affect the above as requested.

3.18 Contractor Purchases: The contractor shall make reimbursable purchases, as required by individual TOs during performance. Material and Other Direct Costs (ODC) are not subject to profit, but may include applicable indirect expenses. Prior to purchases, the contractor shall verify and state that sufficient funds have been provided in the ODC CLIN, justify purchase, and submit the request for approval. The Contractor shall obtain advance TO COR validation and KO approval for ODCs equal to or greater than the micro-purchase threshold as defined IAW FAR 2.101, at least two weeks prior to the date the required purchase is needed. Contractor shall obtain advance TO COR approval for ODCs less than the micro-purchase threshold, at least two weeks prior to the date the required purchase is needed. Prior to purchase, the contractor shall show proof of competition for all purchases over the micro-purchase threshold and document why the recommended source was selected. The contractor shall also complete a Justification and Approval (J&A) as required by FAR Subpart 6.3 for all non-competitive (sole source) and brand name only purchases, and include a copy of the justification in the approval package.

3.18.1 The contractor shall implement procedures for Item Unique Identification (IUID) of Government Property IAW DFARS 252.211-7007 purchased under this contract. The contractor shall mark legacy parts and equipment listed in each TO, mark new parts and equipment acquired under TO's, as required, and update DoD IUID Registry for required parts and equipment. The contractor shall use fully compliant Unique Item Identifier (UII) to maximum extent possible for covered equipment purchased on this contract.

4.0 DELIVERABLES:

4.1 Reports and Data Deliverables: The contractor shall deliver all reports and data described in the paragraphs below. Additional deliverables may be specified in each TO. Deliverables shall be submitted in electronic media via e-mail. The electronic media used shall be compatible with current versions of Microsoft (MS) Word, Excel, and PowerPoint. Paper copies will be provided by exception only.

4.1.1 Monthly Performance and Cost Report (MPCR):

Purpose: This report provides current status and projected requirements of funds, Direct Productive Person Hours (DPPH), and work completion and is used by the Government to manage funds and evaluate contractor progress.

Format: The report shall be in contractor format in MS Excel, when not specified by the KO. The initially used format arrangement shall be used for all subsequent submissions. Any change in format after the initial submission must be approved by the KO.

Content: The Performance and Cost Report shall contain the following:

Man-hours: Total man-hours expended by technical categories or program tasks, cumulative total man-hours to date, and percentages of total man-hours spent to date. On non-service order related TOs, state whether or not remaining hours are sufficient to complete the task. NOTE: For service-order related TOs, while the contractor and KO are working towards an acceptable format, the contractor is allowed to submit in their preferred format.

Funds: Total funds expended, by task, for the month: cumulative total funds spent to date; and percentage of total contract funds spent to date. On non-service order related TOs, state whether or not remaining funds are sufficient to complete the task. ODC and travel costs in same format, but separate worksheet, from labor costs. NOTE: For service-order related TOs, while the contractor and KO are working towards an acceptable format, the contractor is allowed to submit in their preferred format.

The report shall include both numeric and graphical comparison (line graph) of projected hours and actual hours, projected costs and actual costs, and an Estimate at Complete for each month and cost category. NOTE: This section is not required on service order related TOs.

Frequency: Monthly – Submissions shall be on the 15th calendar day of the month following the period being reported (or next immediate workday if submission date falls on a federal holiday or weekend.

Distribution: KO – 1 copy
COR – 1 copy
TO COR for Applicable TO – 1 Copy

4.1.2 Monthly Status Report (MSR):

Purpose: This report provides the status of contractor effort towards achieving contract objectives. It identifies accomplishments for the month, difficulties encountered and problems resolved. It compares the status achieved to planned goals and the resources expended for the month. It is used by the Government to monitor and evaluate contractor performance.

Format: The report shall be in contractor format in MS Word, when not specified by the KO. The initially used format arrangement shall be used for all subsequent submissions. Any change in format after the initial submission must be approved by the KO. The data indicated below shall be contained on a title page or on the first page of the report.

a. Title/identification of the report.
b. Period covered by the report.
c. Date report was prepared.
d. Contract number.
e. Preparing activity or contractor's title.
f. Security classification, when required.

Content: The report shall provide a written explanation, by task order or special project, of the work performed during the month. At a minimum include the following:

Title – Title of the task order or special project and the task order number.

Summary of Monthly Activity – A narrative of the:

- Overall task order/project status.

- Status of each milestone/task as defined by the statement of work or contract and whether or not the task order/project is on schedule, if not, the effort planned to meet the schedule.

- Major problems/deficiencies encountered, the impact of those problems, and resolution or recommended solutions.

- Anticipated problems and their effect on the overall work effort/project and steps taken to remedy problem situations.

- Significant tasks/technical activities initiated or completed.

- A narrative of outstanding problems existing as of the previous status report, and their resolution status.

- Status of deliverables.

- A list of employees who completed PII training, the completion date, and a list of employees who have not had the training.

- Any other information deemed important by the contractor.

Frequency: Monthly – Submissions shall be on the 15th calendar day of the month following the period being reported (or next immediate workday if submission date falls on a federal holiday or weekend.

Distribution: KO – 1 copy
COR – 1 copy
TO COR – 1 Copy for each TO COR per task order

4.1.3 Limitation on Subcontracting Report:

Purpose: This report provides the Government information regarding contractor adherence to the 50 percent rule IAW FAR 52.219-14, Limitations on Subcontracting and 13 CFR 125.6. This report will enable the Government to ensure the prime contractor is meeting this requirement (1) individually, or (2) together with other small business members of a formal joint venture, or (3) together with a small number of small business subcontractors forming an informal joint venture.

Format: The report shall be in contractor format in MS Excel, when not specified by the KO. The initially used format arrangement shall be used for all subsequent submissions. Any change in format after the initial submission must be approved by the KO. The data indicated below shall be contained on a title page or on the first page of the report.

- **a.** Title/identification of the report
- **b.** Period covered by the report.
- **c.** Date report was prepared.
- **d.** Contract number.
- **e.** Preparing activity or contractor's title.
- **f.** Security classification, when required.

Content: For the purpose of calculating the cost of contract performance incurred for personnel of prime contractors and subcontractors or consultants, the following costs shall apply:

- (**1**) Direct Labor Dollars
- **(2)** Direct Labor Overhead Dollars
- **(3)** General and Administrative Dollars on Direct Labor and Direct Labor Overhead

When the Contractor is found to be under the 50% rule IAW FAR 52.219-14, Limitations on Subcontracting, they will provide a summary of a plan to ensure adherence to FAR 52.219-14 by the end of the Basic Contract period of performance.

Frequency: Quarterly – Submissions shall be on the 15th calendar day of the first month of each calendar year quarter (15 Jan, 15 Apr, 15 Jul, 15 Oct) following the end of the reporting period or next immediate workday if submission date falls on a federal holiday or weekend.

Distribution: KO – 1 copy
COR – 1 copy

4.2 Documents or reports produced by the contractor as deliverables for this contract or TO's shall become the property of the Government upon acceptance. Deliverables will not be the contractor's proprietary information and shall not be marked as proprietary data.

5.0 PERFORMANCE ASSESSMENT:

5.1 The Performance Requirements Summary (PRS) is a list of performance objectives and performance thresholds that will be regularly verified by Government personnel. Each performance objective represents a significant performance criteria required in the PWS by the Government at the time of contract award. The performance threshold represents the minimum acceptable level of performance. The performance objectives and performance thresholds represent only the significant tasks of this contract and do not excuse the contractor from performance of other responsibilities identified in this PWS. Performance objectives will be monitored regularly by Government TO CORs. Performance objectives may be added at the basic contract and/or TO level and performance thresholds may be raised or lowered during the course of this contract, but the following objectives will be required for all TO's, at a minimum.

5.2 Performance Requirements Summary:

PEFORMANCE OBJECTIVE	PWS PARAGRAPH	PERFORMANCE THRESHOLD
Objective 1: Provide timely response to time-sensitive requirements, including short notice requirements and a large number of requirements in a short period (surge capability).	**2.1 & 2.11**	Contractor receives no more than one formal customer complaint/ contract discrepancy report per year for all TOs. Contractor provides 90% of TO Proposals within 7 business days or KO-approved extension.

Objective 2: Compliance with DD254, Contract Security Classification Specification, to include proper handling, storage, transmission, and destruction of classified materials.	**2.9**	No security violations.
Objective 3: Contractor performs tasks within proposed funding and notifies KO and COR, in writing, when significant overruns or underruns are incurred.	**4.1.1, 4.1.2**	100% of expected cost overruns are identified to the KO and TO COR PRIOR to submitting the MPCR. For each TO, cumulative cost overruns are less than 3% from budget. 100% of applicable MSRs recommend solutions to any overruns.

5.3 Performance Deficiency Notification: There are two types of deficiency notifications: verbal notification and Performance Assessment Report (PAR). Verbal notification is primarily used for non-repeat, minor discrepancies or tasks that can be re-performed. A PAR will be issued to the contractor by the KO when previous verbal notifications failed to result in corrective actions or when severe deficiencies exist. The PAR will be forwarded to the KO through the COR and TO COR for action. Performance deficiencies may include any Government-identified noncompliance with contract requirements that specifies that an activity or action did not take place, or did not take place to the standards of timeliness or quality required. Note that while the contractor will be given the opportunity for re-performance when possible, significant deficiencies will nevertheless be documented.

6.0 GOVERNMENT QUALITY ASSURANCE (QA): The Government shall establish and document a process to assess contractor performance in all areas of the contract. For the contract the COR and TO CORs will develop and maintain a Quality Assurance Surveillance Plan (QASP) and provide QA to ensure performance results and products meet the standards established. An additional QASP specific to a TO may also be required. Government personnel will be available for technical exchanges with the contractor, will provide technical input, answer questions, review completed work and provide feedback regarding TO efforts.

7.0 GOVERNMENT FURNISHED EQUIPMENT (GFE), PROPERTY, MATERIALS, SERVICES & INFORMATION:

7.1 There is no Government Furnished Property (GFP) or GFE assigned to the contractor at the contract level. GFP/GFE may be provided for performance of individual TOs.

7.2 When the TO requires the contractor to work in a government facility, the Government may furnish or make available working space, equipment and network access. Individual TOs will specify exactly what will be provided. GFP/GFE, materials, and information will remain the property of the Government and will be returned to the TO COR upon request or at the end of the TO PoP.

APPENDIX ~ A ~

ACRONYMS

ACS:	Access Control Systems
AIS:	Automated Information System
AR:	Army Regulation
AT:	Anti-Terrorism
ATCTS:	Army Training Certification Tracking System
ATO:	Anti-Terrorism Office
CAC:	Common Access Card
CCTV:	Closed-Circuit Television
CD:	Compact Disk
CFR:	Code of Federal Regulations
CIMS:	Command Information Management System
CLIN:	Contract Line Item Number
CONUS:	Continental United States
COOP:	Continuity of Operations Plan
COR:	Contracting Officer's Representative
CSU:	Channel Service Units
DFARS:	Defense Federal Acquisition Regulation
DISA:	Defense Information Systems Agency
DoD:	Department of Defense
DoDD:	DoD Directive
DoDI:	DoD Instruction
DPPH:	Direct Productive Person Hours
DVS:	DISA Video Services
ESS:	Electronic Security Systems
FAR:	Federal Acquisition Regulation
FPCON:	Force Protection Condition
FWC:	Future Warfare Center
FY:	Fiscal Year
GCMS:	Government Contractor Monitoring Station
GFE:	Government Furnished Equipment
GFP:	Government Furnished Property
GMD:	Ground-based Midcourse Defense
HQDA:	Department of Army Headquarters
IAW:	In Accordance With
IDIQ:	Indefinite Delivery Indefinite Quantity
IDS:	Intrusion Detection Systems
IGF:	Inherently Governmental Functions
IM:	Information Management

IMA:	Information Mission Area
IMSS:	Information Management Support Services
IS:	Information System
IT:	Information Technology
IUID:	Item Unique Identification
J&A:	Justification and Approval
JFTR:	Joint Federal Travel Regulation
KO:	Contracting Officer
LAN:	Local Area Networks
MPCR:	Monthly Performance and Cost Report
MS:	Microsoft
MSR:	Monthly Status Report
NLT:	No Later Than
OCONUS:	Outside the Continental United States
ODC:	Other Direct Costs
PAR:	Performance Assessment Report
PBX:	Private Branch Exchange
PCs:	Personal Computers
PII:	Personal Identifiable Information
PMP:	Project Management Professional
POC:	Point of Contact
PRS:	Performance Requirements Summary
PWS:	Performance Work Statement
QA:	Quality Assurance
QASP:	Quality Assurance Surveillance Plan
QC:	Quality Control
QCP:	Quality Control Plan
ROC-H:	RTS Operations Center-Huntsville
RMF:	Risk Management Framework
SCI:	Sensitive Compartmented Information
SCIF:	Sensitive Compartmented Information Facility
SF:	Standard Form
SMDC:	Space Missile Defense Command
TDY:	Temporary Duty Station
TO:	Task Order
TO COR:	Task Order Contracting Officer Representative
TS:	Top Secret
UII:	Unique Item Identifier
UL:	Underwriters Laboratories
U.S.:	United States
USAKA-RTS:	US Army Kwajalein Atoll-Reagan Test Site

USASMDC/ARSTRAT:	U.S. Army Space and Missile Defense Command/Army Forces Strategic Command
USSTRATCOM:	United States Strategic Command
VTC:	Video Teleconference
WAN:	Wide Area Network
WAWF:	Wide Area Workflow